УДК 004.4

ДИСТАНЦИОННОЕ ОБРАЗОВАНИЕ - ЗАЩИТА АВТОРСКИХ ПРАВ

Д.А. Степанян[1]

1 *diana14.02.94@mail.ru*; Кубанский государственный университет, г. Краснодар

Рассмотрена реализация защиты авторских прав на базе дистанционного образования.

Ключевые слова: дистанционное образование, авторское право.

Дистанционное образование — самостоятельная, относительно новая и довольно перспективная форма обучения, реализуемая в основном с помощью информационно-телекоммуникационных сетей. Дистанционное образование предполагает взаимодействие учителя и ученика на расстоянии.

Данная форма образования имеет ряд преимуществ. Так, с ее помощью нет необходимости преодолевать большие расстояния для получения необходимых знаний, можно изучать курсы в удобное время, а также предоставляется широкий выбор образовательных курсов и специальностей.

Порядок применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ утвержден приказом Министерства образования и науки Российской Федерации от 9 января 2014 г. № 2[1].

При построении дистанционного обучения необходимы средства, обеспечивающие следующие функциональные возможности:

- средства администрирования;
- средства разработки учебных курсов;
- средства передачи материалов курса;
- средства синхронной и асинхронной связи;
- средства мультимедийного преподавания;
- средства оценивания успеваемости студентов.

Система дистанционного обучения — это комплекс программно-технических средств, описанных выше.

В настоящее время количество разработанных платформ дистанционного обучения приближается к двумстам. К наиболее используемым принадлежатMoodle, eLearning Server, Blackboard, WebCT Campus Edition, WebCT Vista, IBM Lotus LearningSpace, WebTutor, Sakai, Доцент, Прометей, Орокс и другие. Для всех этих платформ является общим то, что они соответствуют основным и общепринятым в мире требованиям и стандартам организации дистанционного обучения. То есть они доступны, персонифицированные, модульные, просты в использовании, интерактивные, адаптированные, соответствуют требованиям компьютерной безопасности.

К системе дистанционного образования предъявляются следующие требования безопасности и секретности материалов:

- аутентификация студентов;
- аутентификация преподавателей;
- конфиденциальность персональных данных студентов и преподавателей;
- защита доступа к экзаменам;

- целостность данных, конфиденциальность хранения и защита результатов экзаменов;
- конфиденциальность связи между студентом и преподавателем;
- защита авторских прав учебных курсов.

Остановимся более подробно на последней проблеме.

Учебные курсы дистанционного образования считаются ценным имуществом, принадлежащим организации или преподавателю и их хищение вполне возможно. Причем необходимо защитить материалы курса от несанкционированного копирования во время хранения, передачи или, непосредственно, в момент просмотра урока.

В связи с бурным развитием технологий мультимедиа остро встал вопрос защиты авторских прав и интеллектуальной собственности, представленной в цифровом виде. В связи с этим разрабатываются различные меры защиты информации, организационного и технического характера. Один из наиболее эффективных технических средств защиты мультимедийной информации заключается во встраивании в защищаемый объект невидимых меток - цифровых водяных знаков.

Название этот метод получил от всем известного способа защиты ценных бумаг, в том числе и денег, от подделки. В отличие от обычных водяных знаков цифровые знаки могут быть не только видимыми, но и невидимыми. Невидимые анализируются специальным декодером, который выносит решение об их корректности. Цифровые водяные знаки могут содержать некоторый аутентичный код, информацию о собственнике, либо какую-нибудь управляющую информацию.

Цифровой водяной знак (ЦВЗ) - специальная метка, незаметно внедряемая в изображение или другой сигнал с целью тем или иным образом защищать информацию от несанкционированного копирования, отслеживать распространение информации по сетям связи, обеспечивать поиск информации в мультимедийных базах данных.

Классификация стеганографических систем на основе ЦВЗ

В зависимости от того, какая информация необходима детектору для выявления ЦВЗ, стегосистемы ЦВЗ делятся на три класса: открытые, полузакрытые и закрытые системы.

Таблица 2.1. Классификация стеганографических систем на основе ЦВЗ

Вид систем внедрения ЦВЗ		Что требуется детектору		Выход детектора	
		Исходный сигнал	Исходный ЦВЗ	Да / Нет	ЦВЗ
Закрытые	Тип I	+	+	+	-
	Тип II	+	-	-	+
Полузакрытые		-	+	+	-
Открытые		-	-	-	+

Различают три типа ЦВЗ:

1. Робастные;
2. Хрупкие;
3. Полухрупкие.

Устойчивость ЦВЗ к различным воздействиям на заполненный контейнер называют робастностью.

Робастные ЦВЗ имеют применение в некоторых задачах, поэтому требования к ним ставятся в зависимости от цели их внедрения.

Категории требований к робастным ЦВЗ:

1. ЦВЗ обнаруживается всеми желающими. Сообщает о владельце защищаемого контента и предназначается для предотвращения ненамеренного нарушения авторских прав;

2. ЦВЗ обнаруживается, хотя бы, одной стороной. Применяется для поиска незаконного распространения копий, к примеру, в сети Интернет;

3. ЦВЗ крайне тяжело модифицировать или извлечь из контейнера. Предназначается для аутентификации.

Эти требования противоречивы и их одновременное выполнение невозможно. Поэтому в различных приложениях используются как системы ЦВЗ с секретным, так и с общедоступным ключом.

Хрупкие ЦВЗ разрушаются при небольших изменениях контейнера-результата и применяются для аутентификации сигналов. В отличии от средств электронной подписи, хрупкие ЦВЗ все же разрешают некоторую модификацию контента. А так же, хрупкие ЦВЗ должны не только определить факт изменения контейнера, но также установить его вид и местоположения

Полухрупкие ЦВЗ устойчивы к одним воздействиям и неустойчивы к иным. Вообще говоря, все ЦВЗ можно отнести к этому типу. Тем не менее полухрупкие ЦВЗ преднамеренно создаются таким образом, чтобы быть неустойчивыми к изменениям определенного рода.

Информацию об авторстве учебного курса можно вставить в кадр видеоурока.

Рассмотрим встраивание ЦВЗ в изображение.

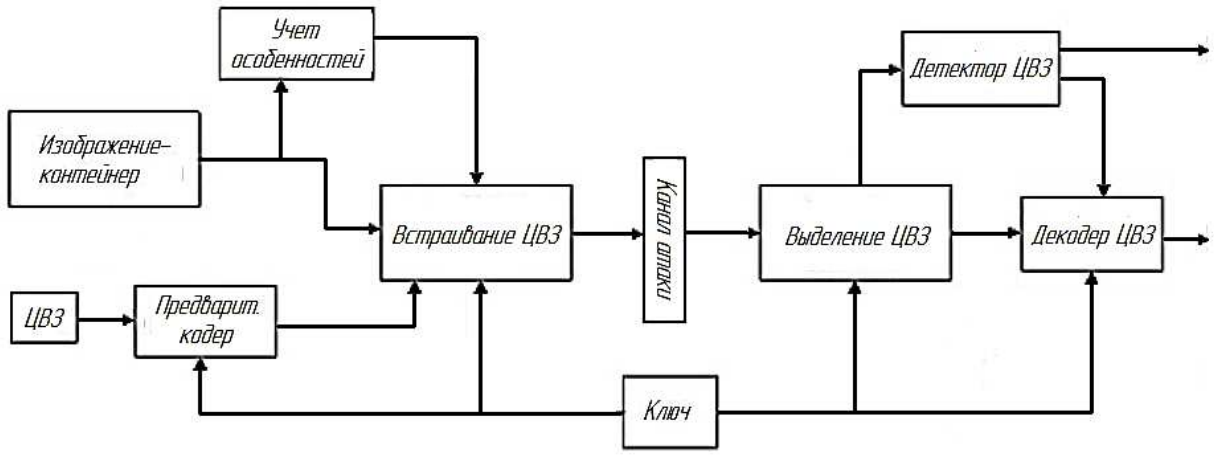

Рис. 1. Структурная схема типичной стегосистемы ЦВЗ

Все современные алгоритмы стеганографии должны обеспечивать устойчивость встраиваемых ЦВЗ. В частности, контейнеры с внедренными ЦВЗ должны предусматривать вероятность сжатия контейнера любым из методов. В связи с этим, также как и алгоритмы сжатия изображений, стегоалгоритмы должны учитывать особенности человеческого зрения, и использовать те же преобразования, что и в современных алгоритмах сжатия. Исходя из этого, вложение информации производится либо в пустой контейнер, либо в процессе сжатия исходного изображения, либо в уже сжатое алгоритмом изображение.

Сжатие понимается, как сокращение количества бит, необходимых для цифрового представления изображений. Сжатие основывается на уменьшении статистической и психовизуальной избыточности. Статистическая избыточность может быть пространственной (корреляция между соседними пикселями), либо спектральной (корреляция между соседними частотными полосами). В алгоритмах сжатия обнуляются не пиксели изображения, а спектральные коэффициенты. Достоинство такого подхода состоит в том, что спектральные коэффициенты близкие к нулю имеют склонность располагаться в наиболее ожидаемых областях, что приводит к появлению длинных серий нулей и повышению эффективности кодирования. Значимые коэффициенты подвергаются более или менее точному квантованию и также сжимаются кодером длин серий. На последним этапе алгоритма сжатия применяется энтропийный кодер (Хаффмана или арифметического).

Для оценки качества восстановленного изображения используют либо меру среднеквадратического искажения, определяемую как

$$СКО = \frac{1}{N}\sum_{i=1}^{N}(x_i - \hat{x}_i)^2,$$

где N - число пикселей в изображении, $x_i, \hat{x}_i$- значение пикселей исходного и восстановленного изображений.

Либо применяется модификация этой меры - пиковое отношение сигнал/шум, определяемое как

$$ПОСШ = 10\log_2 \frac{N \cdot 255^2}{\sum_{i=1}^{N}(x_i - \hat{x}_i)^2},$$

где 255 - максимальное значение яркости полутонового изображения (т.е. 8 бит/пиксель). Восстановленное изображение считается приемлемым, если $ПОСШ \geq 28/30$ дБ (в среднем).

Часто используется принцип встраивания данных, когда сигнал контейнера представлен последовательностью из n бит. Скрытие информации начинается с определения стегопути (биты контейнера, изменения которых не приводит к заметным искажений). Далее, в соответствии с ключом, среди этих бит выбираются биты, заменяемые битами ЦВЗ.

Алгоритмы встраивания данных в пространственной области

Преимуществом алгоритмов встраивания данных в пространственной области является то, что ЦВЗ внедряется в области исходного изображения и не нужно выполнять вычислительно громоздкие линейные преобразования изображений. ЦВЗ внедряется за счет манипуляций яркостью $l(x, y) \in \{1, ..., L\}$ или цветовыми составляющими $(r(x, y), g(x, y), b(x, y))$.

Большое количество алгоритмов встраивания ЦВЗ в пространственную область изображений основаны на использовании широкополосных сигналов (ШПС). Основная идея применения ШПС в стеганографии заключается в том, что данные внедряются в шумовой сигнал малой мощности. Так как сигнал малой мощности, то для защиты ЦВЗ применяют помехоустойчивые коды.

Алгоритмы встраивания данных в области преобразования

В алгоритмах сжатия используется тот факт, что большая часть энергии изображений сконцентрирована в низкочастотной части спектра. Поэтому необходимо произвести декомпозицию изображения на субполосы. Стегосообщение добавляется к субполосам изображения. Для вложения сообщения используются среднечастотные субполосы спектра изображения в которых шум изображения примерно равен шуму обработки.

Низкочастотные субполосы носят шумовой характер, а высокочастотные субполосы подвержены воздействию различных алгоритмов обработки (шум обработки).

Для сжатия изображений эффективно применение вейвлет-преобразования и ДКП, потому что они хорошо моделируют процесс обработки изображения в СЧЗ, отделяют «значимые» детали от «незначимых». Их целесообразнее применять в случае активного наруши-

теля, так как модификация значимых коэффициентов может привести к неприемлемому искажению изображения.

Технические средства защиты авторских прав (ТСЗАП; англ. DRM — Digital rights management) признаются любые технологии, технические устройства или их компоненты, контролирующие доступ к произведению, предотвращающие либо ограничивающие осуществление действий, которые не разрешены автором или иным правообладателем в отношении произведения.

«DRM» - аббревиатура от английского выражения «digital rights management», и означает управление цифровыми правами.

Основной функцией DRM является защита работ от копирования и всевозможных действий, запрещаемых правообладателями на основании авторского или смежных прав после продажи конечному пользователю.

По законодательству Российской Федерации запрещен обход любых технических средств защиты авторских прав.

Большое количество нынешних систем DRM основаны на крипто стойких методах защиты. Эти методы сформированы на предположении, что для получения доступа к зашифрованной информации правомерному обладателю копии необходим секретный ключ. Такой подход сводит к нулю всю защиту. Поэтому системы DRM пытаются спрятать от пользователя применяемый ключ шифрования.

Литература

1. Об образовании в Российской Федерации: Федеральный закон от 29.12.2012 № 273-ФЗ (ред. от 03.07.2016).

2. Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ: приказ Минобрнауки России от 09.01.2014 № 2.

3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 13.07.2015 № 263-ФЗ с изм. и доп., вступ. в силу с 10.01.2016).

4. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014 № 242-ФЗ с изм. и доп., вступ. в силу с 01.09.2015).

5. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 28.11.2015, с изм. от 30.12.2015).

6. Агарновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ / Агарновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. - М.: Вузовская книга,2009.

7. Rogers P. Encyclopedia of Distance Learning / P. Rogers, G. Berg , J. Boettcher, C. Howard, L. Justice, K. Schenk. - 2 edt., 4 vol. - New York-Hershey: IGI Global, 2010.

DISTANSE EDUCATION – COPYRIGHT PROTECTION

D.A. Stepanyan

The implementation of the copyright protection process was considered on the basis of distance education.

Keywords: distance education, copyright.